

SCHEME OF ENCRYPTION FOR BLOCK CIPHERS AND MULTI CODE GENERATION BASED ON SECRET KEY

P. Anuradha Kameswari^{*}, R. Chaya Kumari and L. Praveen Kumar

Department of Mathematics, Andhra University, Visakhapatnam - 530003,
Andhra Pradesh

panuradhakameswari@yahoo.in, chayakumari.divakarla@gmail.com,
lavudi.5686@yahoo.co.in

ABSTRACT

In this paper we propose a scheme of encryption for Block ciphers in N -alphabet, where every member of any m -block of plain text is enciphered by different permutations which are generated by the help of a secret key word. Further we extend this method to multicode encryption using the fact that encrypting each member differently is the basis of multicode encryption.

KEY WORDS Encryption, Block cipher, Multicode encryption

1. INTRODUCTION

The philosophy of modern cryptanalysis is based on Kerchoff's principle stated as 'The security of cryptosystem must not depend on keeping the crypto-algorithm secret rather it should depend only on keeping the key secret'. In this principle, the sender communicates the secret key or keys to the intended recipient over a secured channel before the message being interchanged. When the sender and the recipient agree upon the secret key or keys, they start communicating with each other. This type of cryptosystem is called a Private Key cryptosystem [1, 8].

The private key cryptosystem is classified into three categories namely, Monoalphabetic cryptosystems, Polyalphabetic cryptosystems and Transposition systems [11]. A cryptosystem is called Monoalphabetic when the message units are single letter blocks. The shift cryptosystem, affine cryptosystem and the substitution cryptosystem are the monoalphabetic cryptosystems.

Let P and C denote the numerical equivalents of plaintext and cipher text message units respectively and K denote the key space in a cryptosystem. In the Shift Cryptosystem for an N -alphabetic, we have $P = C = K = \square_N$. For each k in K the encryption function $e_k(x): P \rightarrow C$ and the decryption function $d_k(x): C \rightarrow P$ are defined as

^{*} Corresponding Author
DOI : 10.5121/ijnsa.2011.3610

$$e_k(x) \equiv x + k(\text{mod}N)$$

$$d_k(y) \equiv y - k(\text{mod}N).$$

In the affine cryptosystem for an N-alphabetic, we have $P = C = \mathbb{Z}_N$ with

$$K = \{ (a, b) \in \mathbb{Z}_N \times \mathbb{Z}_N ; (a, n) = 1 \}$$

and for each k in K, the encryption function and decryption function are defined as

$$e_k(x) \equiv ax + b(\text{mod}N)$$

$$d_k(y) \equiv a^{-1}y - a^{-1}b(\text{mod}N).$$

In the substitution system in N-alphabetic, we have $P = C = \mathbb{Z}_N$ and for the key space $K = S_N$, the symmetric group on N-symbols and for each π in K , the encryption function and decryption function are defined as

$$e_\pi(x) = \pi(x)$$

$$d_\pi(y) = \pi^{-1}(y).$$

All the above systems can be broken by using frequency analysis. It is observed that in order to make these systems more secure it is to be made that each letter in the cipher text should appear with equal frequency. Basing on this rule polyalphabetic cryptosystem is constructed. Vignère System, Auto-key cipher system and Hill cipher are some of such polyalphabetic cryptosystems. All these cryptosystems are dealt in general under block ciphers, where the block ciphers are cryptosystems in which blocks of a fixed length are encrypted as blocks of same length with the encryption and decryption functions being permutation functions. The block ciphers are used for the encryption of long documents using the modes of operation like Electronic Code Book mode (ECB mode) [7, 10], the Cipher Block Chaining mode (CBC mode), Cipher Feed Back mode (CFB mode), Output Feed Back mode (OFB mode) [2, 6]. In this paper we propose a scheme of encryption for Block ciphers in N-alphabet, where every member of any m-block of plaintext is enciphered by different permutations which are generated by the help of a secret key word presented in a theorem in section 2 and the extension of the method to multi code encryption is given in section 3.

2. AN ENCRYPTION SCHEME FOR BLOCK CIPHERS

In this section we give an encryption scheme for block ciphers in an N-alphabet that is determined by a private secret word which provides different permutations in encrypting each member of the plaintext in the following theorem.

Theorem Let P and C be the set of all numerical equivalents of plain text and cipher text message units respectively. If the plain text and cipher text message units are of m - blocks in an N- alphabet, for a secret word of same length m there is a permutation π_i in S_N associated to numerical equivalent k_i of i^{th} alphabet of any block of the plain text that generates a function e from P to C given as $e(P_r) = \pi_i(P_r) + rk_i$ for all $r \equiv i(\text{mod}m)$ is an encryption

function with decryption function $d(C_r) = \pi_i^{-1}(C_r - rk_i)$. Thus leading to an encryption of each character of any m-block by different permutation.

Proof: Let $P = C = \square_N^m$ and let (k_1, k_2, \dots, k_m) be the numerical equivalent of the private secret word agreed upon then define the function $\Pi : \{k_1, k_2, \dots, k_m\} \rightarrow \mathbf{S}_N$ by $\Pi(k_i) = \pi_i$ for $\pi_i \in \mathbf{S}_N$ given as $\pi_i = (k_i, 2k_i, \dots, rk_i, (r+1)k_i, 0)(l_1, l_2, \dots, l_i)$ for each rk_i taken modulo N and

$$\{l_1, l_2, \dots, l_i\} = \{1, 2, \dots, N-1\} - \{k_i, 2k_i, \dots, rk_i, (r+1)k_i, 0\}$$

with the property $l_1 < l_2 < \dots < l_i$. If P_r is any r^{th} member of m-block of a plain text then $e(p_r) = \pi_i(p_r) + rk_i$ where $r \equiv i \pmod{m}$ is an enciphering transformation with deciphering transformation $d(C_r)$ given as $d(C_r) = \pi_i^{-1}(C_r - rk_i)$ for C_r be any r^{th} character of any m block in ciphertext [4, 5].

Example : The above encryption scheme is described for a block of length 8 in the alphabet {A,B,C,...,Z} and the word "ENCIPHER" is taken to be the secret word. The numerical equivalent of the secret word is given as (4,13,2,8,15,7,4,17), and the permutations π_i associated to the numerical equivalents obtained are as follows :

- $\pi_1 = (4, 8, 12, 16, 20, 24, 2, 6, 10, 14, 18, 22, 0)(1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25)$
- $\pi_2 = (13, 0)(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25)$
- $\pi_3 = (2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 0)(1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25)$
- $\pi_4 = (8, 16, 24, 6, 14, 22, 4, 12, 20, 2, 10, 18, 0)(1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25)$
- $\pi_5 = (15, 4, 19, 8, 23, 12, 1, 16, 5, 20, 9, 24, 13, 2, 17, 6, 21, 10, 25, 14, 3, 18, 7, 22, 11, 0)$
- $\pi_6 = (7, 14, 21, 2, 9, 16, 23, 4, 11, 18, 25, 6, 13, 20, 1, 8, 15, 22, 3, 10, 17, 24, 5, 12, 19, 0)$
- $\pi_7 = \pi_1$
- $\pi_8 = (17, 8, 25, 16, 7, 24, 15, 6, 23, 14, 5, 22, 13, 4, 21, 12, 3, 20, 11, 2, 19, 10, 1, 18, 9, 0)$

The above permutations are used in the encryption of any plain text. The encryption of the plain text 'CRYPTOGRAPHY' is given in the following table:

P_r	N.E. of P_r	$\pi_k(P_r)$	rK_i	$\pi_k(P_r) + rk_i \pmod{26}$	C_r	
C	2	$\pi_1(2) = 6$	4	10	K	
R	17	$\pi_2(17) = 18$	26	44	S	←
Y	24	$\pi_3(24) = 2$	6	8	I	
P	15	$\pi_4(15) = 17$	32	49	X	
T	19	$\pi_5(19) = 8$	75	83	F	
O	14	$\pi_6(14) = 21$	42	63	L	
G	6	$\pi_7(6) = 10$	28	38	M	

R	17	$\pi_8(17) = 8$	136	144	O	←
A	0	$\pi_1(0) = 4$	36	40	O	
P	15	$\pi_2(15) = 16$	130	146	Q	
H	7	$\pi_3(7) = 9$	22	31	F	
Y	24	$\pi_4(24) = 6$	96	102	Y	

The plain text ‘CRYPTOGRAPHY’ is enciphered as ‘KSIXFLMOOQFY’. Similarly the plain text ‘AN ATTEMPT TO BREAK A CIPHER’ is enciphered as ‘IAIBFBSMFUMVTFMNUDLZJH’.

Remark 1 : Each member of any m-block is encrypted by different permutations. This provides unconditional security to the cryptosystem. This encryption scheme is determined by the secret key word agreed upon. The secrecy of the cryptosystem is maintained as long as the sender and the recipient maintained the secrecy of the key word. This may be attained by key exchange using public key exchange cryptosystem [12, 16].

3. A SCHEME FOR GENERATING MULTI-CODES IN MULTI-CODE ENCRYPTION:

For the encryption of data [3, 15] with multi-codes for one character, each character is allotted a certain number of multi-codes. If a_1, a_2, \dots, a_m are m-codes for a character c in a plain text, c is represented by the code a_i in the cipher-text if the occurrence number o_c of c is such that $o_c \equiv i \pmod{m}$. In this section we give a method of generating multi-codes for each character in multi-code encryption which can be deciphered, by the receiver with the knowledge of secret key word that is agreed upon. The multi-codes for each of the character are generated through a secret key by the following procedure:

- Select a secret sentence of **m** words each of length **n** as secret key.
- Using the secret sentence, codes called **Basic codes** are introduced.
- Using numbers 1, 2, 3... n the codes called fundamental **codes** are introduced.
- The **multi - codes** are generated by modifying the fundamental codes with basic codes.

4. Construction of Basic codes and Fundamental Codes:

Basic Codes: Let S be the secret sentence of **m** words each of length **n** in N-alphabet i.e. $S = (w_1, w_2, \dots, w_m)$, and for each word w_i in the sentence, let a_i^j be the number in which the numerical equivalent of the j^{th} alphabet in \square_N is taken modulo 9, then the numerical equivalent of w_i is $a_i^1 a_i^2 a_i^3 a_i^4 \dots a_i^n$. Now the mn basic codes arranged in a block of m columns and n rows are generated as follows:

$$\begin{matrix}
 B_{11} B_{21} B_{31} B_{41} \dots B_{m1} \\
 B_{12} B_{22} B_{32} B_{42} \dots B_{m2}
 \end{matrix}$$

$$\begin{matrix}
 B_{13}B_{23}B_{33}B_{43} \dots B_{m3} \\
 B_{14}B_{24}B_{34}B_{44} \dots B_{m4} \\
 \vdots \\
 B_{1n}B_{2n}B_{3n}B_{4n} \dots B_{mn}
 \end{matrix}$$

where B_{ij} is a code of length m given as

$$B_{ij} = B_{ij}^1 B_{ij}^2 B_{ij}^3 \dots B_{ij}^m$$

with

$$\begin{aligned}
 B_{ij}^1 &= \begin{cases} a_i^j & \text{for } i = 1 \\ a_i^j + B_{i-1}^{m-1} + B_{i-1}^m & \text{for } i > 1 \end{cases} \\
 B_{ij}^2 &= B_{i-1}^m + B_{ij}^1 \\
 B_{ij}^3 &= B_{ij}^1 + B_{ij}^2 \\
 B_{ij}^m &= B_{ij}^{m-2} + B_{ij}^{m-1}
 \end{aligned}$$

Note : The additions performed throughout in the generation of all the codes are the repeated digital sums i.e. digital root **dr** where the digital root of a number is the single digit value obtained by an iterative process of summing digits, on each iteration using the result from the previous iteration to compute a digit sum [6]. The process continues until a single-digit number is reached. Digital roots can be calculated with congruences rather than by adding up all the digits, by the following formula:

$$\mathbf{dr}(n) = \begin{cases} n(\bmod 9) & \text{if } n \neq 0 \pmod{9} \\ 9 & \text{if } n \equiv 0 \pmod{9} \end{cases}$$

Fundamental Codes : If the secret sentence is of m words each of length n, then the fundamental codes are taken to be all possible n^m arrangements of the n numbers {1, 2, ..., n} in m places, that is the set F of all fundamental codes is given as

$$F = \{F_k : F_k = F_k^1 F_k^2 F_k^3 \dots F_k^m \text{ where } F_k^i \in [1, 2, 3, \dots, n] \text{ for all } i=1, 2, 3, \dots, m\}$$

Now as

$$n^m = nm.t + r \text{ for some } t, r \in \mathbb{N} \text{ with } 0 \leq r < nm$$

the set F may be partitioned into t number of disjoint subsets of nm elements and the nm elements of each such subset are arranged in a block of m columns and n rows as that of the basic code block.

Multi – Codes : The multi-codes are generated by modifying each block of the fundamental codes by basic code block as follows : For any positive integer $1 \leq s \leq t$ if $F_{s_{ij}}$ is the ij^{th} entry of the s^{th} fundamental code block and B_{ij} is the ij^{th} entry of the basic code block the multi code $M_{s_{ij}}$ of length m is given as

$$M_{s_{ij}} = M_{s_{ij}}^1 M_{s_{ij}}^2 \dots M_{s_{ij}}^m \text{ for } M_{s_{ij}}^k = B_{ij}^k + F_{s_{ij}}^k \text{ for all } k=1, 2, \dots, m$$

Example : Let the sentence ‘THIS TEXT MADE EASY’ of 4 words each of length 4 be the secret sentence agreed upon. In this example we have $m = 4 = n$. Using the given secret

sentence the corresponding Basic codes are computed and represented in a tabular form as follows:

Basic codes			
1123	6966	6393	7189
7753	3696	6393	3696
8876	9663	3696	6393
9999	1123	9336	6393

The **fundamental codes** formed with the numbers 1, 2, 3, 4 are arranged in 64 rows which are categorized into 4 blocks and each block consisting of 4 sub blocks and each sub block consisting of 16 codes. The fundamental codes are then used to generate the multi - codes for 64 characters. The multi-codes are generated by modifying each block of the fundamental codes by basic code block. For any positive integer $1 \leq s \leq 16$ if $F_{s_{ij}}$ is the ij^{th} entry of the s^{th} fundamental code block and B_{ij} is the ij^{th} entry of the basic code block the multi code $M_{s_{ij}}$ of length 4 is given as

$$M_{s_{ij}} = M_{s_{ij}}^1 M_{s_{ij}}^2 M_{s_{ij}}^3 M_{s_{ij}}^4 \text{ for } M_{s_{ij}}^k = B_{ij}^k + F_{s_{ij}}^k \text{ for all } k=1, 2, 3, 4.$$

The Multi codes generated for the 64 characters $\{A, B, \dots, Z; a, b, \dots, z; 0, 1, 2, \dots, 9; + \text{ and } -\}$ are given in the table below:

CHARACTER	MULTICODES				CHARACTER	MULTICODES			
A	2234	7187	7434	8231	g	4234	9187	9434	1231
B	8865	4728	7435	4748	h	1865	6728	9435	6748
C	9989	1786	4739	7446	i	2989	3786	6739	9446
D	1114	2247	1461	7447	j	3114	4247	3461	9447
E	2334	7287	7534	8331	k	4334	9287	9534	1331
F	8965	4828	7535	4848	l	1965	6828	9535	6848
G	9189	1886	4839	7546	m	2189	3886	6839	9546
H	1214	2347	1561	7547	n	3214	4347	3561	9547
I	2434	7387	7634	8431	o	4434	9387	9634	1431
J	8165	4928	7635	4948	p	1165	6928	9635	6948
K	9289	1986	4939	7046	q	2289	3986	6939	9646
L	1314	2447	1661	7647	r	3314	4447	3661	9647
M	2534	7487	7734	8531	s	4534	9487	9734	1531
N	8265	4128	7735	4148	t	1265	6128	9735	6148
O	9389	1186	4139	7746	u	2389	3186	6139	9746
P	1414	2547	1761	7747	v	3414	4547	3761	9747
Q	3234	8187	8434	9231	w	5234	1187	1434	2231
R	9865	5728	8435	5748	x	2865	7728	1435	7748
S	1989	2786	5739	8446	y	3989	4786	7739	1446
T	2124	3247	2461	8447	z	4114	5247	4461	1447
U	3334	8287	8534	9331	0	5334	1287	1534	2331
V	9965	5828	8535	5848	1	2965	7828	1535	7848
W	1189	2886	5839	8546	2	3189	4886	7839	1546
X	2214	3347	2561	8547	3	4214	5347	4561	1547
Y	3434	8387	8634	9431	4	5434	1387	1634	2431
Z	9165	5928	8635	5948	5	2165	7928	1635	7948

a	1289	2986	5939	8646	6	3289	4986	7939	1646
b	2314	3447	2661	8647	7	4314	5447	4661	1647
c	3534	8487	8734	9531	8	5534	1487	1734	2531
d	9265	5128	8735	5148	9	2265	7128	1735	7148
e	1389	2186	5139	8746	+	3389	4186	7139	1746
f	2414	3547	2761	8747	-	4414	5547	4761	1747

The multi codes given in the table can be used in enciphering any plain text. The multi code encryption has its own advantages as seen in the encryption of the plain texts ‘CRYPTOLOGY’ and ‘cryptology’ given as follows:

CRYPTOLOGY	9989	9865	3434	1414	2124	9389	1314	1186	9189	8387
Cryptology	3534	3314	3989	1165	1265	4434	1965	9387	4234	4786

Remark 2 : The basic codes and the fundamental codes constructed as above generate the multi - codes $M_{s_{ij}}$ that are distinct for all $i = 1,2, \dots m, j = 1,2, \dots n$ and $s = 1,2,\dots t$ and are used in the allotment of multi-codes for nt number of characters. The set of any given $n \cdot t$ characters may be divided into ‘ t ’ subsets and for any $1 \leq s \leq t$ the j^{th} character in s^{th} subset is allotted the ‘ m ’ multi-codes $M_{s_{1j}} M_{s_{2j}} \dots M_{s_{mj}}$.

Remark 3 : In this encryption each member of the plain text is encrypted by a different code and the multi codes generated are determined by the secret key which is a secret sentence agreed upon. The security in this encryption is maintained as long as the secrecy of the secret key is maintained. This may also be attained by a regular change of the secret key by using the public key exchange cryptosystem [13, 16].

5. Conclusion:

An encryption scheme is breakable if a third party without prior knowledge of the key can systematically recover plaintext frame. An encryption scheme can be broken by exhaustive search of the key space. So to make this approach computationally infeasible, one may enhance the key space. The key space for the proposed scheme has $N!^m$ elements.

The encryption scheme proposed is a block cipher consumed with the stream cipher idea of processing character by character where a key stream $(\pi_1, \pi_2, \dots, \pi_m)$ is generated by using secret key word of length m , π_i used for all $r \equiv i \pmod{m}$, unlike the vernam's one time pad. The information of the plaintext cannot be easily obtained as the π_i 's are symmetric functions in S_N in an N -alphabet and the encryption function modifies the π_i by rk_i increasing the average period of the key stream.

The Multicodes can be generated by using a secret sentence both by the sender and the receiver. The secrecy of the multicodes is maintained as long as the sender and the recipient maintain the secrecy of the key word. This may be attained by key exchange using public key exchange cryptosystem.

References

- [1] A. K. Bhandari "*The public key cryptography*" *proceedings of the advanced instructional workshop on Algebraic number theory, HBA (2003)287-301.*
- [2] J. Buchmann "*Introduction to cryptography*", Springer-Verlag 2001.
- [3] Firas Layth Khaleel Al-ameen "*Data encryption using multi-codes for one character*" *IJCNS journal VOL.10 No 9, September 2010.*
- [4] Douglas R. Stinson "*Cryptography theory and practice*" *Second edition.*
- [5] Gerhard Frey "*The arithmetic behind cryptography*" *AMS volume 57, Number 3.*
- [6] Hans Delfs Helmut Knebl "*Introduction to cryptography*" *Principles and its Applications, second edition.*
- [7] Keith M.Martin, Rei Safavi-Naini, Huaxiong Wang and Peter R.Wild "*Distributing the encryption and decryption of a block cipher*".
- [8] Neal Koblitz "*A course in number theory and cryptography ISBN 3-578071-8, SPIN 10893308*".
- [9] I.Niven, H.S. Zuckerman and J.H.Silverman "*An Introduction to the Theory of Numbers*", 5th ed., John Wiley and Sons, New York, 1991.
- [10] Phillip Rogaway Mihir Bellare John Black Ted Krovetz "*OCB: A block-cipher mode of operation for efficient authenticated encryption*".
- [11] R.Thangadurai "*Classical Cryptosystems*" *proceedings of the advanced instructional workshop on Algebraic number theory, HBA (2003)287-301.*
- [12] P.Rogaway,M-Bellare,J.Black,T-Korvetz "*A Block Cipher mode of operation for efficient authenticated encryption*" *Eighth ACM conference on computer and communication security (CCS-8) ACM Press, 2001.*
- [13] K.H.Rosen "*Elementary number theory and its applications*" *Third edition, Addison-Wesley.*
- [14] Serge Vaudenay "*A classical introduction to cryptography applications for communication security*" *Springer International Edition.*
- [15] William Stallings "*Cryptography and network security principals and practice*" 5th ed.
- [16] Harry Yosh "*The key exchange cryptosystem used with higher order Diophantine equations*" *IJNSA VOL.3, No.2, March 2011.*
- [17] Zuckerman, I.Niven and Hugh L.Montgomery "*An Introduction to the Theory of Numbers*", 5th ed., Wiley Student Edition.

Authors

Author 1 : Dr. P.Anuradha Kameswari is working as Assistant professor in the Department of Mathematics , Andhra University, Visakhapatnam, Andhra Pradesh, India. Her research interests are Algebraic Number Theory, Number Theory and Cryptography.

Author 2: Ms. R.Chaya kumari has completed her M.Sc., M.Phil and presently pursuing Ph.d in the Department of Mathematics , Andhra University, Visakhapatnam, Andhra Pradesh, India. Her area of research is Number Theory and Cryptography.

Author 3: Mr. L.Praveen kumar has completed his M.Sc. and presently pursuing Ph.d in the Department of Mathematics , Andhra University, Visakhapatnam, Andhra Pradesh, India. His area of research is Number Theory and Cryptography.